Office of the Governor
State Chief Information Officer

Security Policy and Guidelines

Title: Information Technology Risk Management Policy with Guidelines

Purpose: To ensure that state agencies manage risks appropriately. Risk management includes the identification, evaluation, and control of risks associated with an agency's business, information technology infrastructure, the information itself, and physical security to protect the state's information technology assets and vital business functions.

Scope: This policy applies to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services." Use by local governments, LEAs, community colleges, constituent institutions of the University of North Carolina and other public agencies is encouraged to the extent allowed by general statutes.

POLICY STATEMENT

The State of North Carolina recognizes that each agency, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens. The risk management program must identify and classify risks and implement risk mitigation as appropriate. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

GUIDELINES

Agencies are encouraged to select and use guidelines that support industry best practices for risk management relative to business continuity planning and security as appropriate. Some suggested guidelines are listed below.

Risk Management Program Activities:

Agency risk management programs should focus on the following four types of activities:

- **Identification of Risks:** A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
- **Analysis of Risks:** An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
- **Mitigation Planning:** Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For important risks, mitigation plans should be developed.

- **Tracking and Controlling Risks:** Collecting and reporting status information about risks and their mitigation plans, responding to changes in risks over time, and taking corrective actions as needed.

Business Continuity Risk Management Processes: For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt agency business. Agencies should identify the potential impacts in order to develop the strategies and justify the resources required to provide the appropriate level of continuity initiatives and programs.

Agencies should conduct business risk impact analysis activities that:

- Define the agency's critical functions and services.
- Define the resources (technology, staff, and facilities) that support each critical function or service.
- Identify key relationships and interdependencies among the agency's critical resources, functions, and services.
- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
- Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimate financial losses over time of each critical function or service.
- Estimate tangible (non-financial) impacts over time of each critical function or service.
- Estimate intangible impacts over time of each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority. (For example - tax filing dates, reporting deadlines, etc.)
- Identify any critical non-electronic media required to support the agency's critical functions or services.
- Identify any interim or workaround procedures that exist for the agency's critical functions or services.

Security Risk Process: The focus of security risk management is an assessment of those security risk outcomes that may jeopardize agency assets and vital business functions or services. Agencies should identify those impacts in order to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical agency functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize agency critical functions and services.

Security risk impact analysis activities include the:

- Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.
- Identification of any due diligence requirements for agency functions or services.

- Identification of confidential information stored in the agency's files and the potential for fraud, misuse, or other illegal activity.
- Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical agency functions and services.
- Identification of the processes used to monitor and report to management on the IT Security infrastructure. (Baseline security reviews, review of logs, use of ID's, logging events for forensics, etc.)
- Identification of the agency's IT Change Management and Vulnerability Assessment processes.
- Identification of what security mechanisms are in place to conceal agency data (Encryption, PKI, etc.)

AUTHORITY

The State CIO is authorized to adopt this policy. G.S. §147-33.110.